# ATTACHMENT H

## STATE OF MARYLAND DATA SECURITY POLICY

**Date:** August 16, 1999
**Distribution:** Agency Data Systems Security Officers

## STATE POLICY: INFORMATION PROCESSING RESOURCES SECURITY

I. Authority

A. Governor's Executive Order 01.01.1983.18, which created the State Data Security Committee to establish State data security standards.

B. State agency information system security practices as enumerated by the State Data Security Committee.

C. Article 27, Sections 45A and 146 of the Annotated Code of Maryland.

II. Objective

A. The purpose of the Policy is:

1. To assign responsibility, on an agency/institution-wide basis, for implementing the procedures required by the State Policy issued by the State Data Security Committee.
2. To protect the integrity of the State agency and institution computerized record systems.

B. This policy is applicable to all units of the Executive Branch of State Government.

III. Policy Statement

In recognition of the fact that information is a valuable resource in the efficient operation of State government at all levels, and the fact that the privacy of individuals is directly influenced by the collection and use of personal records, it is the policy of the State of Maryland to protect sensitive data from unwarranted disclosure and to protect information processing resources from abuse or damage by natural or other causes.

The following procedures shall be adhered to by all agencies within the Executive Branch of Maryland State Government.

IV. Procedure

Each agency administrator, head of a commission and the other directing authority of State Government 1) shall be responsible to formulate directives to properly protect information processing resources in accordance with the State Computerized Record System Security Requirements and the requirements and recommendations contained therein, and 2) appoint a Security Officer as required by the Governor's Executive Order.

## I. State Agency Data Systems Security Practices

### A. Agency Computer Software and Records Security

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for all computer systems including mainframes, minicomputers, data communications facilities, local area network (LANs) file servers, microcomputer network nodes, and standalone microcomputers (desktops or notebooks/portables) which contain critical or sensitive data files. (Management must identify what are critical or sensitive data files).

1. Written procedures to safeguard application system data files must be prepared and followed.

2. The documentation for each application system must address sufficient controls for maintaining the security of source documents, before, during, and after the data entry process, and the distribution of all output.

3. All source and object programs must be maintained in a manner which prevents unauthorized access.

4. Each agency is required to maintain a list of its data processing applications and files.

5. Each agency is required to store copies of agency computer files and programs on a routine basis at an off-site location. An off-site location must be in a building other than the one that houses the primary computer files and programs.

6. Each agency is required to store at an off-site location copies of data systems documentation which would be vital in continuing the operation of the systems in an emergency situation which has resulted in the destruction of the original documentation.

7. When capabilities are available, each agency must use an automated method (e.g., a security software package) to safeguard application system data files.

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED in all instances where agencies have standalone microcomputers (desktops or notebooks/portables) or LAN file servers and microcomputer network nodes.

8a. Because notebook/portable microcomputers are highly susceptible to theft, the devices must be protected via the use of access-control software, passwords and a boot or power-on password where feasible and practical. A power-on or boot password protects the device from use of a DOS or system bootable diskette to bypass the computer's access control software.

8b. The storage of network modem telephone numbers and network passwords in unsecured standalone microcomputers (desktops or notebook/portables) is strictly forbidden.

9. All agency software and files on removable media must be put into a locking storage unit when not in use or be maintained in areas that are locked when not in use.

10. To minimize the chance of computer viruses being introduced into microcomputers only authorized and properly licensed personal computer software packages are to be used on PC's. Authorized PC software packages are those developed and approved by agency management or those obtained from reliable and responsible vendors, e.g. State software BOA vendors, nation-wide distributors, etc. that are committed to assuring product quality. The use of unauthorized or unlicensed PC software and programs (i.e., software obtained from computer bulletin boards, friends, other employees, etc.) is strictly forbidden. Only work related PC software approved by agency management is to be installed on State microcomputer equipment.

11. As a means of recovering from a computer virus attack or disaster, backup procedures must be implemented on a routine basis for agency software and files stored in PCS and LANs.

12. All users of microcomputers must use a virus scan/protection program on a regular basis to minimize damage caused by virus attacks and to scan data files for viruses entering the computer. All virus scan/protection programs used for this process must be updated on a regular frequency. The frequency of the updates is a minimum of every two years.

13. All employees utilizing personal computers must sign the State of Maryland Software Code of Ethics Form (part of the Department of Budget and Management's Policy Number 95-1) which states that unauthorized duplication of copyrighted computer software violates the law and is contrary to the State's standards of conduct.

14. When a sensitive or critical PC application is created, the application author is responsible for documenting the application. Documentation may differ slightly from one type of application to another; however, all documentation must contain the following elements:

- ♦ a written description of the application;
- ♦ step by step instructions on how to use the application;
- ♦ the names and the location of the PC files;

- a copy of the output;
- the backup procedure for the application.

The following documentation is suggested:

- a log of revisions (the log should include the name of the application, the original author, the date it was created, the date of each revision, the name of the individual who revised the application, and the reason for the revision).

15. A written plan to assure that all its critical and sensitive applications are "Year 2000" compliant must be adopted by each agency by December 31, 1997. Security software supporting those critical and sensitive applications must be "Year 2000" compliant.

16. A written PC security policy must be promulgated and adopted by each agency. This policy must include, as a minimum, items A.8. through A.15 above.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

Security should be considered in the design and development of each computerized record system. All agency programs should be maintained in a library which provides an audit trail of changes made to the programs. Wherever appropriate, each document which is used for initiating error corrections to computer records should contain a statement of justification and proper authorizations.

Agencies are encouraged to tie standalone PC's together into a Local Area Network (LAN) so that software can be loaded and managed centrally, critical and sensitive files can be stored and backed up more easily and sensitive files and applications can be more readily protected from virus attacks and other security threats.

B. Agency Computer Hardware Security

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED in all instances where agencies have standalone or network microcomputers, notebook/portable microcomputers and computer terminals located in areas other than within secured computer facilities.

1. Agencies must take appropriate preventative actions to guard against damage to, or theft of, these devices.
2. Because notebook/portable microcomputers are highly susceptible to theft, none of these devices are to be left in unsecured areas while not in use e.g., the back seat of a parked vehicle.

3. Computer terminals, standalone microcomputers and microcomputer network nodes must not be left logged on to computer systems when unattended.

4. When capabilities are available, computer terminals and microcomputer network nodes must be automatically logged off by the operating system when there is no terminal activity for a pre-designated period of time.

5. When disposing of microcomputer processing units, an agency must take the appropriate action to delete all of the data that is contained on the processing unit's hard drive.

6. In a telecommuting environment, an agency must provide the same level of security on the microcomputer used at home as the microcomputer used in the workplace.

C. Password, Sign-on and Access Security

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for State agencies which utilize remote connectivity and data communications capabilities.

1. Individual user passwords must be used for every session, transmission or access to application systems.

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for State agencies where password, sign-on or access control security features are installed.

2. Passwords must be changed periodically.

3. The assignment of passwords must be tightly controlled.

4. Users must be advised that all passwords must be kept confidential and secure. The procedure for assigning passwords must reflect that efforts are made to retain the confidentiality of passwords.

5. Terminal and microcomputer network node users of the computer facilities must be restricted to accessing only files that they are individually authorized to access and also be limited to authorized operations that they may perform on or with these files.

6. System administrators must maintain a formal, written audit trail of all security access control activities on the system. The audit trail shall include, but not be limited to maintaining a log of all changes to all user access rights/logonid's and requests to change user passwords as long as the user access rights/logonid's are active on the system; maintaining a log of all deleted user access rights/logonid's for at least two years or until audited by the Legislative Auditor and maintaining a log of all security exceptions/violations for at least two years or until audited by the Legislative Auditor.

7. Agency management or a designee of agency management must periodically review and document the security privileges, data file and program access control rights of all personnel authorized to interface with critical or sensitive application systems, files and programs. Agency management personnel that perform this review task must not include persons who manage the access controls. The review documentation must be retained for at least two years or until audited by the Legislative Auditor.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

Password management software that allows system administrators to define the rules governing how users pick their passwords is available. Use of these systems strengthens data security significantly. With appropriate password management, administrators can specify that 1) passwords are not actual names or words, 2) are of a minimum and maximum length, 3) are not used over again, 4) contain at least one number, and 5) are not composed of repeating digits. Adequate password management also permits the development of special password validation programs for processing unique applications. It is therefore recommended, where capabilities exist, that administrators implement all or some of the aforementioned password management techniques to improve password security.

Also, it is important to ensure that users are who they say they are when they sign-on to a system. This includes incorporating the ability to check users authorization every time they access a new system resource. Software is available that are aimed at identifying possible intruders and preventing unauthorized entry into systems. Recommended features include 1) preventing a single user from signing on to more than one workstation at a time; 2) restricting individual users to workstations with specific addresses; and 3) scheduling capabilities that lets administrators specify the times of day when users are allowed to sign-on to a system. It is therefore recommended, where capabilities exist, that administrators use the aforementioned sign-on techniques to the maximum extent possible.

D. Agency Information Technology Personnel Practices

These required and recommended security practices apply to all employees (contractual and permanent) and information technology consultants who interface with application systems that have been identified by agency management as being critical or sensitive. The types of duties or functions of personnel addressed by the foregoing shall include, but not be limited to security officers who grant system access rights to others, programmer-analysts, systems programmers, database administrators, network managers, information technology consultants and other personnel identified by agency management who have rights to access critical or sensitive application systems, files and programs.

THE FOLLOWING SECURITY PRACTICE IS REQUIRED.

All agency security officers must satisfactorily complete a course of instruction specified by the State Data Security Committee.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

1. It is recommended that each agency have a designated Certified Software Manager. A Certified Software Manager is defined as an individual who has participated in the Certified Software Manager Course Certification Exam program offered by the Software Publisher's Association (SPA) through its outsourcing provider, Fortress Technologies, at an approximate cost of $400 per person. The one day, 6-hour course is designed for managers and specialists working in the areas of MIS, microcomputing, computer services and technical support in addition to auditors, counsel, and others responsible for software compliance. The course defines the skills necessary to be a Certified Software Manager so an individual can
gain the full benefits of software and avoid the legal penalties of mismanaging it. By successfully completing the course an attendee will:

   - understand copyright law and licensing agreements;
   - understand the software audit process;
   - understand the benefits and processes of software asset management;
   - develop a workable software management plan.

   Once attendees have completed the course, they must pass a one-hour exam in order to be certified. The exam will be administered by Sylvan Prometric for an additional $100 fee that may be paid directly to Sylvan. The exam must be scheduled after the course is taken.

   Course materials attendees will receive include the following:

   - A 300-plus page comprehensife student guide
   - SPA's anti-piracy video, posters, brochures and article reprints
   - SPAudit software to accelerate the self-audit process saving staff time
   - "A Road map for Buying Software" poster and guide

   SPA offers the one day course during the year in Washington D.C. In order to receive a current schedule of course dates, agencies can contact the SPA at the following address:

Http.//www.spa.org

2. If, in the opinion of agency management, a prospective employee will be interfacing with a sensitive or critical computer application, a criminal history record check should be conducted.

NOTE: A criminal history record checking service is offered, at a fee, to state agencies by the State of Maryland's Department of Public Safety and Correctional Services (DPSCS). The procedure for this service is entitled "Criminal History Record Checks For Prospective State Employees". Request forms which must be signed by the appointing authority of a state department or agency are available from:

Customer Service Unit
CJIS Central Repository
P.O. Box 5743
Pikesville, Maryland 21208-0195
Phone #: 410-318-6021

State agencies are encouraged to hire applicants on a conditional basis pending receipt of the satisfactory criminal history record check.

Background checking should be performed for final candidates for these positions prior to selection for employment. Background checking is contacting previous employers, references, and other appropriate individuals or organizations to verify the education, training and/or experience needed to meet minimum qualifications.

Agency personnel with access to critical or sensitive data files should be advised periodically as to how data security violations should be reported. Whenever feasible, employees that work with security sensitive computerized record systems should be periodically rotated in their job functions. Agency data systems security procedures which pertain to agency personnel should also apply to temporary and contractual personnel.

To provide appropriate degrees of internal control over data processing operations, agency management should segregate functions so that information technology personnel who perform systems maintenance functions are not performing user type functions as a regular part of their duties and responsibilities. In addition, agency management should separate the following data processing duties and responsibilities among several employees:

- Performing computer operations functions,
- Maintaining application program software,
- Maintaining operating systems and databases and

- Performing data processing security functions.

## II. State Computer Facility Security Practices

This section applies to all State mainframe, minicomputer, data communications facilities and Local Area Network (LAN) installations that process critical or sensitive data files. (Management must identify what are critical or sensitive data files).

A. Physical Security of Computer or Data Communications Operations Area

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED.

1. All fire safety devices must be approved and periodically checked by the State Fire Marshal.

2. The facility must have a written procedure for the disposal of its own data processing materials.

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED only at computer facilities with separated, restricted computer or data communications operations areas.

3. The facility is required to control the access to the computer or data communications operations area, permitting entry of authorized personnel only. Entry of maintenance and custodial personnel must be controlled. Former employees and visitors to the computer operations or data communications area must always be escorted.

4. If a building with a separate facility has security guards, these guards are to be scheduled to make routine checks of the facility. Management must identify the level of routine checking to be performed by security guards (e.g., perimeter checking only, full physical access, visual inspection, etc.).

5. If security guards are not available, an access alarm is to be used when the facility is unattended.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

When the size or schedule of the computer or data communications facility does not permit all employees to be known and recognized, every employee should be required to display an official identification containing a photograph of the employee.

The computer or data communications operations area should contain smoke and/or heat sensors for early detection of a fire. An automatic fire-suppressing system should be installed. The space under any raised flooring should be inspected periodically for possible hazards.

Some types of network protocol analyzers and test equipment are capable of monitoring (and some, of altering) data passed over the network. Use of such equipment should be tightly controlled since they emulate terminals and can monitor and modify sensitive information, or contaminate data.

B. Contingency Planning

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED.

1. The computer or data communications facility management must routinely assess the relative probability of significant hazardous events occurring at the facility. As a minimum, a significant hazard means fire, flood, unauthorized entry or access, power failure and man made (e.g. terrorist) or natural disasters.

2. The computer or data communications facility management must routinely assess the vulnerability of the facility to the specified significant hazards.

3. The computer or data communications facility management must have a contingency plan which addresses and prescribes actions to be taken for all significant events which management has determined could place the facility at risk. Specifically, the contingency plan must address personnel, hardware, software, data, remote connectivity, and data communications networks. The plan also must contain a section dealing with the recovery from a major disaster that would render the facility unusable and require restarting operations at an alternate site. The major disaster recovery section must address the initial response, restart procedure, personnel assignments, backup resources and facilities, and emergency vendor contacts/vendor agreements.

4. The computer or data communications facility management must periodically validate the contingency plan. The following guidelines, listed in priority order, are to be used in conducting the validation:

   a) Actual, live, full scale disaster recovery test exercises must be used wherever feasible and practical or,

   b) Partial recovery test exercises or simulations (e.g. tabletop exercises) of disaster recovery procedures must be used when it is impractical to conduct full scale disaster recovery tests.

   The computer or data communications facility management must periodically update the contingency plan to reflect deficiencies noted during validation tests and to assure that the plan is current, viable and complete.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

As an aid in securing upper management's support for on-going contingency planning efforts, the computer or data communications facility management should consider performing a risk analysis which will assist in striking an economic balance between the impact of risks and the cost of protective measures. A well executed risk analysis will improve security awareness, identify assets, significant hazardous events and controls, improve the basis for decisions and justify expenditures for security. Risk analysis steps include the following:

- Identify critical information assets;
- Determine significant hazardous events;
- Estimate likelihood of occurrences of significant hazardous events;
- Document the impact of a loss of critical information assets (compute annual loss expectancy);
- Identify applicable cost associated with controls to be implemented;
- Project annual savings of controls.

During the assessment of the contingency plan, the computer or data communications facility management should consider the merits of having arrangements for alternative computer processing capabilities at an off-site location for emergency needs. If this option is cost effective and practical, a formal agreement should be prepared with the organization responsible for the off-site facility.

Contingency planning in Client Server environments is more complicated than it is for a mainframe data center. Many Client Server systems utilize technologies produced by several vendors in a distributed computing environment, thus multiple points of failure may occur which can magnify the scope and severity of problems. An agency's Client Server disaster recovery plan is best managed by centralized information technology systems groups.

To plan for unseen calamities, the computer or data communications facility management should determine where critical Client Server information is stored and how it is used. It is recommended that:

a) Physically distributed servers be pulled back into a centralized, controlled environment wherever feasible or practical to better manage and protect information, improve security, data integrity and asset tracking.

b) Software tools should be employed in Client Server environments to help create ways to protect information and systems. These software tools can help agencies choose what is most essential to recover.

The computer or data communications facility management should consider installing fault tolerant hardware and fault management software features in all critical and sensitive networks and application systems to guard against data loss and to provide for high systems availability.

Network and application system fault tolerant hardware features that agencies should consider installing include, but are not limited to, are:

- Error correction code (ECC) memories;
- Redundant arrays of inexpensive disks (RAID) technologies;
- Hot-pluggable and hot spare disks;
- Dual redundant power supplies sized to support fully loaded configurations and
- Smart uninterruptable power supplies.

Network and application fault management software features that agencies should consider installing include, but are not limited to, the capability to monitor and report on the status of:

- Memory;
- Processors;
- Disk storage devices;
- Power usage;
- Network equipment and
- Internal temperatures of processor units.

C. Computer Records

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED.

1. When capabilities are available, the computer system must provide an audit trail of all authorized and unauthorized attempted accesses to computer resources.

2. When capabilities are available, the computer system must use an automated method (e.g., a security software package) to safeguard computerized files.

D. Remote Connectivity and Data Communications

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for State computer facilities which utilize remote connectivity and data communications.

1. The computer facility must provide procedures to control access from the remote user locations during hours that remote user locations are closed.

2. Each user access must be terminated if the security code is still incorrect after a specific number of user attempts to log on.

3. Before being prompted for the user name and password, a banner must appear warning users of system monitoring procedures and State laws that apply to breaches of computer security. For example:

   **WARNING: Unauthorized access to this computer is in violation of Article 27, Sections 45A and 146 of the Annotated Code of Maryland. This system is being monitored. Anyone using this system expressly consents to such monitoring. Detection of unlawful conduct may be referred to law enforcement officials.**

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED.

User access logs should be regularly reviewed by an individual(s) outside of the computer operations area.

E. Dial-up Line Access

THE FOLLOWING SECURITY PRACTICES ARE REQUIRED for computer facilities which have dial-up communication lines.

1. The computer facility management must control the distribution of the computer telephone number used for a critical or sensitive application system. In these instances, the computer facility procedures for distributing the computer telephone number must reflect that efforts are made to retain the confidentiality of the telephone number.

2. When capabilities are available or can be reasonably acquired, dial-up activity sessions must be terminated when the telephone is hung up or the carrier is dropped.

3. When capabilities are available or can be reasonably acquired, each dial-up connection must be broken whenever an unauthorized attempt is made to access a facility's computer.

4. Any system implemented for the purpose of providing electronic services for the citizens of the State via public dial-in access or through a connection to the Internet should be isolated/protected from an agency's internal computer network. This should be accomplished by ensuring the system has no internal network connection or is protected by a properly implemented network or application level firewall that enforces a responsible access control policy.

THE FOLLOWING SECURITY PRACTICES ARE RECOMMENDED

1. Systems accessible from dial-up terminals are particularly vulnerable to unauthorized access since the call can be initiated from virtually any telephone instrument. Official users of dial-up facilities should be distinguishable from public users if they are to be given access rights greater than those given public users. For services other than those authorized for the public, users of dial-up terminals should be positively and uniquely identifiable and their identity authenticated to the system begin accessed. This should be implemented via a two level security procedure consisting of using either a call back facility or a Public Data Network (PDN) service to access the system. When using a call back facility, official users should be provided an automatic hang-up and call back feature, which calls back to only pre-authorized numbers. When using a PDN service, a separate, network User ID and user address code should be provided to official users by the PDN service. This is in addition to the computer system's User ID and password which is provided and maintained by the computer facility.

2. An agency should exercise a great deal of care in deciding what information can be properly housed on a publicly accessible system. The agency's assistant attorney general should be involved in this decision making process.